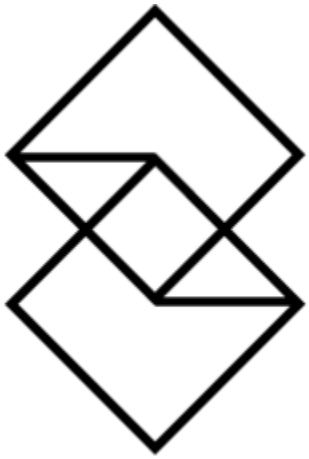

Shift Project

Progress Report

Table of Contents

Q3 2017 – The Release of the Phantom dApp 4

Q4 2017 – The Decentralized Web 5

The Shift IPFS Cluster 6

Jenga 6

Hydra 7

Q1 2018 – White Paper Release and Product Improvements 8

Introductory White Paper 8

Shift IPFS Cluster Update and Custom IPFS Daemon 8

Jenga Update: Stricter Node Monitoring 8

URL Rewriting (Routing) 9

URL Redirecting 9

Custom 404 Error Pages 9

Regex Support for IPFS Rewrites 10

Q2 2018 – Evaluating the Shift Platform 11

Sidechains 11

Consensus Algorithm 14

IPFS Cluster 17

Q3 2018 - Phoenix, Blockchain Integration & Our Pricing Model 18

Phoenix 18

Blockchain Integration 19

Our Pricing Model 20

Q4 2018 – What's to come? 22

This document is intended to provide prospective users and partners with a comprehensive summary of the Shift Project's activities preceding our upcoming release. It contains a detailed summary of the progress the Shift Project has made during the last year, providing the information necessary to understand the background behind the creation of the world's first blockchain-governed, InterPlanetary File System (IPFS) storage and web hosting solution.

Q3 2017 - The Release of the Phantom dApp

We begin our summary in July of 2017, the month in which the Shift Project achieved its most landmark product release up until that point. During that summer, we launched the prototype of our decentralized application (dApp), Phantom, onto the Shift testnet. This first iteration of our custom IPFS storage and web hosting software consisted of an intuitive 'drag and drop' interface for file management over the global IPFS network.

A significant achievement, this provided the global IPFS initiative[1] with a user interface (UI) that it was sorely lacking at the time. Furthermore, Shift's Phantom UI debuted a domain name system (DNS) wizard for pointing top-level domains to the InterPlanetary Name Space (IPNS) record of published content. This made it possible to host static web pages using our gateway, with the additional option of using text (TXT) records to point easily intelligible web addresses to the global peer-to-peer network hash, thus making the content accessible via regular browsers—though doing so sacrifices a degree of censorship resistance due to the possibility of domain blocking.

Unlike that of today, this first prototype of Phantom was connected to the global IPFS network. However, in the interest of establishing our own blockchain-enabled storage ecosystem on the Shift platform, we decided that an objective of creating a private IPFS infrastructure would need to be adopted. The primary reason for switching to a private IPFS-based storage network was that, with our use case of uniting storage users and providers within a revenue model actuated by supply and demand, a private network would allow us to facilitate the presence of persistent storage. Coexisting within a free and global network would mean accepting the heightened risk that content could be wiped by garbage collectors—processes designed to automatically clear disk memory should the availability of space reach a certain threshold—of a provider with no incentive for maintaining it. This was a prospect that the Shift Project could not abide.

[1] https://ipfs.io/

Q4 2017 - The Decentralized Web

Following a difficult August during which we endured the departure of several team members, in September of 2017, having decided that a private IPFS network would be a necessity, we announced a promise to our community. We pledged to deliver, before the end of the year, a second prototype of the Phantom dApp that would be connected to our own storage network, the first version of the Shift IPFS Cluster. During that period, we also had the realization that a new project website was needed. This was because the site at that time lacked sufficient information that described exactly what the Shift Project is trying to achieve. Our desire was to provide a clear explanation of the project's mission, and thus we started thinking about how to define Shift's vision with greater clarity and in a more precise manner than had ever been officially stated before.

At the time, there were two identities that the Shift Project had come to inhabit. The decision to port the project to a Lisk[2] fork in October of 2016, a project that advertises itself as a blockchain application platform, implied an ambition to support dApp development. While this seemed appropriate, given that we sought to develop, in Phantom, the 'perfect' dApp, we did not want to suggest that building a dApp platform was our primary goal. From our perspective, this would make little sense as a business decision as it would put us in competition with projects with far greater funding. Nevertheless, implying that we were primarily working on a storage solution with the additional ability to host web content would have risked making us a perceived competitor of the likes of Filecoin[3], which had recently gained attention for completing an initial coin offering (ICO) in which a record 257 million US dollars was raised. And so, we decided to market ourselves somewhere between these two extremes, as a decentralized, dApp-capable platform with a primary focus on the hosting of websites.

In order to simultaneously highlight our technological accomplishments in addition to more firmly establishing our brand identity, as well as to provide a little motivation, we announced that on top of releasing our own storage cluster, we would host our new website using our own fledgling technology. This would, in the process, make it the first-ever example of a decentralized website with dynamic content, accessible on a regular browser without the use of third-party plugins and incorporating a real top-level domain.

Those months between September and the New Year were some of the hardest we have ever worked, and we labored right up until the very last day of December. Despite the hardship, our efforts paid off, and, in keeping our promise, we were able to make history. We created the foundation of our own storage ecosystem, a **permanent** storage solution that grants the user full control of their own published content (their website), comparable to, if not faster than, the services provided by centralized web hosting platforms.

One may ask, "How was this done?" The release of our new website, using Phantom to host it on the Shift IPFS Cluster, was made possible using three underlying technologies.

[2] https://lisk.io/
[3] https://filecoin.io/

The Shift IPFS Cluster

The Shift IPFS Cluster, that was, at that time, based on the stand-alone client created by Protocol Labs[4] (known as IPFS Cluster), allowed the user to pin content using the principle of a replication factor set, by default, to three. This principle means that once content is published and then pinned, it is copied across the network and stored at three separate locations (nodes) at all times. Due to the content-based nature of IPFS, the peer-to-peer hypermedia distribution protocol assigns data a hash that allows the network to identify content and detect if it is not being served by one or more of the three nodes. In the event that a node is unable to deliver content, another peer within the IPFS Cluster will download the data from the remaining peer(s), returning the total number of available sources to three.

Jenga

The IPFS protocol, while providing a content-based file system, does not offer a decentralized variant of the domain name system that is so integral to the working of today's internet. In order to ensure our website is accessible on regular browsers, we needed to point a domain to its IPNS hash. While we believe that the IPNS hashes of IPFS technology represent a revolution in how the internet is able to function—by granting censorship resistance and the ability to detect if a connection between client and server is lost and content is no longer being served—they do lack a certain degree of user-friendliness. Compatibility with the so-called 'pretty URLs' that we use to access sites is, in our opinion, critical to mass adoption. We thus came to the conclusion that until the development of a decentralized variant of the domain name system comes about, an interim solution is necessary in order to facilitate a transition from the old to the New Web. We therefore created Jenga, a custom-built DNS monitor.

Jenga is responsible for actively inspecting nodes in the cluster to ensure that they are correctly storing pinned content. This is an ongoing process in which an internal list of healthy nodes that are ready to serve content is maintained, guaranteeing that only they are kept in the DNS. Jenga makes published web content resistant against DDoS attacks without sacrificing a pre-existing URL. In this way, Jenga allows Phantom to bridge the Old Web (HTTP/DNS) and the New (IPFS/IPNS), facilitating: real top-level domains, the use of regular browsers without any third-party plugins, and a content-based, peer-to-peer infrastructure.

[4] https://protocol.ai/

Hydra

Hydra is an IPFS-compatible and decentralized content management system (CMS). With the launch of our website, we wanted to offer more than a simple static page. Though with IPFS you can only host static websites, Hydra enables the posting of dynamic content on these sites by storing static JavaScript Object Notation (JSON) data files, or JSON used to pull data from third party APIs. What is more, with Hydra you can easily edit web content without having to rebuild and re-publish the whole site in order to apply these changes. Hydra's capabilities are essential in allowing us to provide support for the storage of application specific data, at least at a small scale, and streamline this data integration.

The completion and deployment of these three integral components by our development team meant that we saw out 2017 with a historic first. It also gave us new ambition and drive to see that 2018 would be no different in being a year of innovation, with much important work yet to be done in achieving our goal of creating a groundbreaking application for the storage and serving of digital media.

Q1 2018 - White Paper Release and Product Improvements

Introductory White Paper

The first month of 2018 concluded with the release of our Introductory White Paper[5], titled: *Phantom: A Decentralized Storage Suite*. With this white paper we wanted to address the problem that Shift's Phantom dApp solves, in addition to describing the architecture of our platform without overburdening the text with unnecessary technical details. Thanks to the assistance of Isabella Dell, the former system architect of Lisk, who, in late-November of 2017, became a Shift advisor, we were able to craft a rich explanatory document that explicated our core ambition: the provision of a groundbreaking storage and web hosting service capable of fundamentally removing the ability of malicious actors to unjustly censor and impede the ethical distribution of legitimate information.

Shift IPFS Cluster Update and Custom IPFS Daemon

Q1 also saw us debut some major changes in the Shift IPFS Cluster following the release of a new version of Protocol Labs' software. Craig C., one of our core developers and Jenga's creator, worked on updating the software in order to remedy issues caused by some of IPFS Cluster's serious bugs, in addition to taking on the task of building a custom IPFS daemon to support URL rewriting (routing), URL redirecting, custom 404 error pages and the implementation of Regex (a superset of wildcards) support for IPFS rewrites.

- **Jenga Update: Stricter Node Monitoring**

  Although in December of 2017 we were very impressed with the Protocol Labs version of IPFS Cluster, we soon started having teething trouble with their software that was, after all, still in 'alpha'.

  There was one issue that proved particularly troublesome. A state began to emerge in which IPFS Cluster was able to host content due to IPFS running, but the cluster would run into issues with pinning. The result was that while Jenga was still able to find content, no new content could actually be pinned to these nodes. What ideally occurs is that when a file is added to and replicated over the cluster, Jenga looks for that file and, if it is able to find it at the required number of DNS nodes, registers that the peers are healthy. Unfortunately, what was happening was that if a peer for any reason disconnected from the cluster due to problems in IPFS Cluster, meaning that new pins could no longer be made to it, Jenga was unable to correctly register that the peer was no longer present, resulting in the return of error 404s for new content. The success of the update Craig implemented lies in the way that it has Jenga pin test files to the cluster at set intervals, therefore confirming that all peers are actually able to deliver newly pinned content.

[5] https://www.shiftproject.com/download/shift-introductory-paper.pdf

- **URL Rewriting (Routing)**

  To further our ambition of making our platform as user-friendly as possible, we saw to it that our inclusion of custom routing allowed us to use, in addition to pretty URLs, ‘pretty path’ functionality (URLs ending in things such as ./team, ./home etc.) and have these paths resolve to the same hash on the server side. It is important to note that IPFS does not offer any way ‘out of the box’ to implement custom routing for hosted websites. This is because when the engineers behind IPFS implemented file serving, they decided against including support for custom routing, instead opting to support routes directly within the folders of content. However, the concept of ‘pretty routes’ is one commonly used within a lot of web frameworks, such as in Apache (a system that most web developers are familiar with), where it is implemented using a configuration file called .htaccess.

  If you wanted to use different URL schemes or do all the routing from a single page in JavaScript, under IPFS you would have to use custom routing or the # found in URLs such as https://ipfs.io/#how. What we have done with our custom IPFS daemon, is allow the site operator to direct ./how to load how.html, or any other file. Our custom IPFS daemon respects that mapping, something that can be seen by browsing our site at, for example, https://shiftproject.com/team, where our custom routing ensures that it works without issue. That we managed to provide this functionality was quite an achievement because pretty URL paths are readable by search engine crawlers. This has the profound effect of enabling search engine optimization (SEO) for any website hosted on our platform.

- **URL Redirecting**

  In a similar manner to URL rewriting, URL redirecting is used to prevent a failure to retrieve content if a page has been relocated. As it is another important aspect of SEO, it was an integral that we include it in our software’s raft of abilities. For example, in January of 2018 we discovered some broken links that came up in Google search results pointing to pages of our previous website. URL redirecting allowed us to correct this issue and remove the possibility of it occurring again.

- **Custom 404 Error Pages**

  Though a largely cosmetic addition, we decided to add support for custom 404 error pages to instances where pages are linked that do not exist. An example of such an error page can be seen at: https://www.shiftproject.com/notfound. This is the customized version of the 404 error page for our own website, that demonstrates how a site operator, rather than relying on the somewhat ‘uninspired’ IPFS default: https://ipfs.io/notfound, is able to set up their own ‘nice looking’ not found page when the case arises in which requested content does not exist.

- **Regex Support for IPFS Rewrites**

  Regex is a superset of wildcards used to denote any character or range of characters in a URL path. Regex support is another functionality that increases the user-friendliness of the Shift platform's hosting capabilities, as IPFS rewrites are a feature that allows one to use pretty URLs that link to custom IPFS paths. Put simply, a user could set a URL path so that any URL that matches ./about/* shows a certain page. In other words, Regex support allows you to map ./file/:id to a certain location, instead of having to map each URL directly. Therefore, rather than having to list ./file/1 ./file/2 ./file/3 etc. in the routes, you can specify one route. This addition was somewhat inspired by .htaccess in Apache, a similarity that will make transitioning to the Shift platform a more streamlined process.

Q2 2018 - Evaluating the Shift Platform

Sidechains

In June of Q2, thanks to a great deal of thought and labor devoted to the task by president and lead developer, Ralf S., we on the Shift Team announced the substantial achievement of being one of the first dApp platforms to have deployed working sidechains. Put simply, sidechains are blockchains that are registered at a mainchain and run in parallel with it, providing a scalability solution for a platform on which decentralized applications are to be run.

To fully explain why we decided to devote time to the task of getting sidechains working, it's necessary to first understand the architecture of the original Crypti/Lisk dApp platform, the project from which our platform was forked. There are essentially three main components within the original Crypti/Lisk design: the blockchain core (mainchain), a sandbox—an isolated Node.js subprocess that may not read the main process, only communicating with it via an application programming interface (API)—and a software development kit (SDK)—a blueprint for all sidechains. These three interact in a particular manner, with the SDK only able to send requests to the sandbox for certain information from the mainchain, while the sandbox replies back to the SDK with the requested information from the mainchain. In other words, communication between the mainchain and sidechain goes through the sandbox and is one-sided. The major advantage of this construction is that if the sandbox for some reason crashes, due to an overloading of the sidechain, the blockchain core (mainchain) keeps running.

While sidechains are not an essential component of our decentralized storage and web hosting solution, we believed that by running our flagship dApp, Phantom, with its own sidechain, we would grant the mainchain an element of protection from subprocesses (such as high-volume content uploads) that might risk overloading it and slowing down transactions. Phantom would also be the perfect example of a dApp with a real sidechain use case, as the sidechain could be used as a decentralized means of governing the private IPFS storage network, while tokens on the sidechain could be used to purchase storage and reward storage providers.

Initially, we intended to leave the task of developing sidechains to Lisk, whose open-source approach would allow us to acquire the code, but, when in November of 2017 Lisk announced that they would not be launching sidechains in the foreseeable future, we decided that, rather than waiting a year or possibly more to fork their code, we would pursue innovation in this potentially useful scalability solution ourselves. So that month, Ralf began work on sidechain development that continued alongside our work on Shift IPFS Cluster and other components of our technology suite. Thanks to his dedication to this complex task, June saw the progress necessary to run fully stable sidechains in a private setting completed. While the SDK was never finished by Crypti, was broken in Lisk 0.9.0, and completely removed within Lisk 1.0.0, Ralf and the Shift Project had made sidechains a reality!

Upon completion, Shift's sidechains were stable and included the following functionalities:

- Block forging, meaning that every forged mainchain block triggers the forging of a sidechain block that is then broadcast to the rest of the sidechain peers.
- Multi-forging, meaning that block forging is set to occur on different sidechain peers running in sync with a consensus factor of at least 51, so that a sidechain delegate is only able to forge when it has consensus with the absolute majority of sidechain block producers.
- Sidechain peers able to synchronize according to a common block lookup.
- Cross-chain token transfers between the mainchain and sidechain (deposits and withdrawals).

Ralf subsequently created and pushed the necessary dApp functionalities to our testnet (and later mainnet) required for the integration of the Phantom dApp with its sidechain. This meant that any dApp, but in our case the Phantom dApp, became extendable with the sidechain SDK related modules required to process sidechain blocks and transactions, ensuring that it can interact with the sidechain.

Owing to us having completed the sidechain code and added the ability to deploy dApps with fully stable and functional sidechains, one might ask "Why have sidechains—or, more specifically, the Phantom sidechain—not yet been released on the testnet?" The principle reason for this at the time was the way token transfers were set up within the sidechain construction of Crypti, where cross-chain transfers are transmitted via an escrow wallet (the wallet of the dApp owner that registered it at the mainchain). We have come to the conclusion that the construction of an escrow wallet is a major liability in respect to the security of token transfers between a mainchain and its sidechains. Before considering running Phantom as a sidechain, we decided it would be necessary to first solve the security issue concerning cross-chain transfers. However, the complexity of this task, discussed in a newsletter[6] we published on the matter, combined with advances made in the Shift Core code outpacing that of the SDK, plus our eagerness to debut our improved storage and hosting functionalities, led us to carefully consider our priorities.

We decided that the most pressing goal of the Shift Project is the release of a decentralized storage and web hosting solution. We therefore concluded that the best course of action, would be opening ourselves up to a new approach. This plan has the storage layer directly integrated with the Shift mainchain, bypassing the entire idea of the Phantom dApp, instead incorporating the aspects of the user interface it provided directly into a rebuilt Shift Nano, our client wallet. Furthermore, integrating our storage and web hosting solution with the principle blockchain also has the advantage of granting greater legitimacy to the SHIFT token. Doing so would mean it acts solely as a means of staking a claim to drive space or as a reward for granting drive space to the Shift network, and not a token that first needs to be transferred cross-chain prior to using it. The token becomes truly one devoted to its utility.

[6] https://www.shiftproject.com/news/news-item/8

An impact of this new course of action that occurred to us, however, was that such an approach inevitably leads one to question the motivation behind our continued use of the Lisk Core, a question granted greater saliency by our reservations about what we consider its flawed consensus system. If Lisk's sidechain functionality (born out of its dominant marketing image as a provider of dApp support), is no longer being used, this leaves the road open for a further evolution in the Shift Project with the provision of faster transactions and greater decentralization in its consensus system. While we have yet to embark fully upon this road, this is a strategy that will see us eventually transition from the Lisk codebase by profoundly re-architecturing the blockchain component of our underlying platform.

Consensus Algorithm

As alluded to in the previous section, another serious conversation we, the Shift Team, had during the second quarter of 2018 concerned the direction to be taken in regards to our chosen consensus algorithm. Already by 2017, issues afflicting the Delegated Proof-of-Stake (DPoS) system we currently use had started to emerge, and participants in the 'cryptocurrency scene' had become vocal in voicing discontent with the controversies that surround it. Foremost among these controversies is the formation and arguably the collusion of so called 'delegate pools', in which delegates that claim to share a certain percentage of their forging reward with voters gain an excessive amount of influence over the network. A key method by which this is achieved is through the implementation of the requirement that to receive a payout for voting for a delegate, an account holder has to vote for all the members of the pool. The prevalence of this strategy became such that delegate pools throughout the various DPoS projects have even been accused of being 'cartel-like'[7] in their behavior, to the extent that purportedly decentralized projects are now centrally controlled.

We have been fortunate in that this phenomenon has not occurred among the Shift Project's forging delegates. Nevertheless, we came to the conclusion that the most effective preventative measure would be proactivity in addressing the root of the issue: the consensus algorithm. Initially, we thought that we could tackle the problems present in DPoS by implementing two minor but highly influential modifications in the way the voting and forging systems work:

1. In respect to voting, we considered amending the attribution of vote weight per account so that it decreases linearly (or logarithmically) in line with the number of votes cast. This would mean that voting for 1 delegate would have proportionally greater influence than if one were to vote for 2, 3 and so on, up to a maximum of 101. The intention behind this would be the weakening of the votes of those engaging in pool voting, while also potentially curtailing the influence of large wallets.

2. The adjustment to the forging system that we considered was more profound. Currently, there are only 101 forging delegates that are each assigned to forge one block per delegate round. As the ranking (and thus the selection) of the forging delegates rarely changes—something unfortunately now prevalent in DPoS projects—we decided that the implementation of a randomizing factor might benefit the network by decreasing this 'entrenchment'. While the number of forging delegates per delegate round would remain 101, our amendment would alter the selection process so that, despite higher ranking delegates having a greater probability of being selected, delegates with a lower rank would be given the opportunity to demonstrate their ability to successfully and reliably forge blocks. This would be owing to the implementation of a random element in selection from a greater total number of candidates than just the top 101 ranking delegates.

[7] https://vitalik.ca/general/2018/03/28/plutocracy.html

> For example, in the case that 226 candidates were eligible for block forging: the first 1-26 (26 delegates) might have a 100% chance of being selected to forge each round, delegates 27-126 (100 delegates) a 50% chance, and delegates 127-226 (100 delegates) a 25% chance. In theory, with the chance of being selected being consistent with a normal distribution, after 4 delegate rounds delegates 1-26 would each have forged 4 blocks, delegates 27-126 each 2 blocks, and delegates 127-226 each 1 block. This model ensures that it is much harder to control an absolute majority (51/101) of the forging delegates within a delegate round, an important factor as a pool group that possesses an absolute majority of the forging delegates within a delegate round could potentially tamper with the database by having their pool's delegates all download an altered snapshot and thereby establish their own leading fork.

While we had announced that such changes would take place in Q1/Q2 of 2018, our discussions with Isabella Dell, who has a great deal of knowledge in this area, led us to conclude that while minor modifications such as these might combat weaknesses in the DPoS system, they would be unable to remedy its core problem: its failure to prevent the emergence of centralizing delegate collusion. Furthermore, they would do nothing to alter the potential issue in which a single person anonymously sets up multiple delegates, claims to share a high proportion of their rewards, and as a result collects the popular vote (and voting weight) necessary to achieve multiple high-ranking forging spots. These are major liabilities that we remain very uncomfortable with, as within any decentralized system it should be statistically impossible for the network to become subject to any one authority, and so we decided to shelve these minor modifications and instead focus our energy on designing an entirely new consensus algorithm.

As we had recruited Rob Ladbrook in the Spring of 2018, an expert in designing complex systems with an ambition to innovate in the field of blockchain, he took on the task of researching and designing a new consensus algorithm that could securely scale to meet the needs of a global file system built to offer hosting features that no other blockchain project currently on the market is able to match. We believe his work will eventually allow us to move away from the problems of DPoS, an algorithm we have increasingly come to consider a single point of failure. For us, security is always number one and this situation has furthered our ambition to design an optimal core that can meet the needs of a global file system and web hosting platform, while also maintaining the lofty goals that make the decentralization movement so compelling.

In order to keep our community informed, we announced that once Rob's research was complete, we would publish his findings as a technical white paper; a blueprint for a complete re-architecturing of the Shift platform. However, when it came to the point at which Rob had completed the general research into the matter, prior to asking him to invest his time in writing up what would need to be a highly-technical document, we sat down to consider the two options available to us. We could stop working on the storage solution using the Lisk-based core and instead devote our time to the technical white paper necessary to start building an entirely new blockchain core and all the necessary accompanying apparatus, or we could shelve it for the time being and focus on releasing the storage and web hosting solution. This would mean retaining the current core for the

present, releasing a functional version of our software suite that would demonstrate our platform's promise, before then re-architecturing from a stronger foundation.

The first of these two options had the obvious downside of meaning that our community would need to wait a very long time to see a working product and our delivery of an actual use case for the SHIFT token. Furthermore, starting work on a complete re-architecturing of the Shift platform would require significantly expanding the Shift Team, needing us to secure and manage greater financial resources. The second option would allow us continue working on our storage and web hosting solution with the current Lisk Core, releasing a functional version capable of demonstrating our token's utility, something our community has long been waiting for. Once done, we could then start development on the new core, having demonstrated the ability to realize our vision of releasing groundbreaking technology. This is something that could then additionally work in our favor by attracting new users, as well as new supporters whose contributions would better enable us to conduct a re-architecturing.

Needless to say, we chose the second option.

IPFS Cluster

Throughout Q2, we on the team were also engaged in extensive testing of Protocol Labs' IPFS Cluster software. In particular, we were pursuing an answer to the question of whether or not its stability was sufficient to make it a viable option for integration with the Shift blockchain. In order to do this while simultaneously maintaining the integrity of the private cluster that we were using to host our website, we set up a second cluster on infrastructure provided voluntarily by several of our forging delegates. As testing progressed, the second cluster was gradually scaled up to approximately 20-30 peers, allowing us to run various scenarios in which peers left the cluster and then attempted to rejoin.

The outcome of this testing was crucial in determining a change in our course of action over the following months. This is because we consistently found that if even a single peer left the cluster incorrectly, the whole cluster would inevitably enter a bad state. What is more, once in a bad state, problems were then amplified owing to the inability of peers to correctly (re)join. The only remedy for the situation once the cluster was in this state, was for the peer that caused the bad state to be manually removed from the cluster via the bootstrap node, and sometimes even this did not work and we were forced to reset the entire cluster. As you may be able to imagine, maintaining a peer-to-peer network consisting of numerous storage node providers under these conditions would have been impossible. The cause of the problem seemed to be a fundamental issue in the way the source code of IPFS Cluster was written, and so we realized that it was one that could not easily or quickly be solved.

In the same manner that we could not tolerate waiting for Lisk's still undelivered sidechains, we decided that we could not leave ourselves dependent upon the work of Protocol Labs to fix its software's fundamental issues. Something that our work on sidechains had also taught us, however, was that correcting errors in the code of others can potentially be more complex and take a greater amount of time than simply building software from the ground up. Furthermore, we realized that having our own IPFS-based storage cluster software would serve us well in the future, as fixing unforeseen problems and optimizing code to suit your own specific use case is far easier when you have designed it yourself. And thus, we decided to start work on our own IPFS-based storage software. With our own, new cluster we would be able to complete what we have wanted since the beginning of the year: a functional, decentralized storage and web hosting solution that is governed by blockchain technology, with the SHIFT token granted utility as a means of claiming storage capacity on the platform.

Q3 2018 - Phoenix, Blockchain Integration & Our Pricing Model

In order to motivate ourselves following our decision to replace Protocol Labs' IPFS Cluster, we set ourselves the ambitious goal of completing the first version of our decentralized storage and web hosting solution and deploying it on the testnet by the conclusion of Q3, 2018. Meeting this goal would require the completion of two principal tasks. First, we would need to code an IPFS-based pin manager as an alternative to the Protocol Labs technology. Second, we would need to integrate the pin manager with the testnet mainchain, allowing a decentralized means of validating the distribution of storage capacity and confirming pin requests in a trustless fashion, while also updating the user interface of our client wallet to support these functions without relying on the no longer needed Phantom dApp.

Phoenix

The first of the three tasks we completed was the IPFS-based pin manager that Craig, its lead developer, named Phoenix. He chose this name because, according to Greek mythology, the Phoenix is a bird to which a long life is attributed owing to its ability to regenerate itself. This alludes to our peer-to-peer storage network's ability to live on, where IPFS Cluster could not. The name is also that of a constellation, a phenomenon that mirrors the relationship between the decentralized nodes that contribute to our network. Not only do constellations depict isolated points granted greater significance through their connection with each other, but they are quite literally an interplanetary network. Our Phoenix is both long-lived and, through its use of the InterPlanetary File System as its peer-to-peer hypermedia distribution protocol, an InterPlanetary network of great significance.

Phoenix, in its guise as the software that needs to be installed and run in order to set up a Phoenix Cluster, is composed of two key components: firstly, Phoenix-core, a custom built peer-to-peer library that facilitates the peer-to-peer messaging layer of Phoenix Cluster and, secondly, Phoenix-cluster, a module that integrates the Phoenix Cluster with the IPFS protocol, creating a second layer on top of Phoenix Cluster called the IPFS swarm. IPFS swarm is the network of digital media storage devices on which content is pinned. Phoenix-cluster allows the peers of the Phoenix Cluster to connect to the swarm and is responsible for the issuing of pin commands to the IPFS swarm peers. Put simply, the Phoenix Cluster functions as the Shift's platform's 'gatekeeper', ensuring that those devices that are a part of the IPFS swarm conform to the prerequisites that we have set for the correct storage of content. This ensures that users of our platform will not need to be concerned that their valuable data could be lost.

The work Craig has completed in this field is a huge achievement on many levels, not least because it was unknown when he began, whether or not the theoretical solutions we together devised would work in practice. Thanks to his dedication, he has now finished work on the first version of Phoenix, one of our key technology offerings, and, since we transitioned the project site over to the first Phoenix Cluster in early October, it has been running healthily and without issue ever since.

Blockchain Integration

The Shift Project is building a platform with which users will be able to use the Shift Nano wallet to access the storage resources of others in order to decentralize their data and web hosting apparatus, as well as grant drive space to the network as storage providers by installing Phoenix. As the provision of drive space requires the deployment and maintenance of software and hardware, which takes time and money, the ecosystem requires a verification system and financial model that is able to monitor and reward participants for satisfactorily granting the services underpinning it. It is the presence of this model that allows the network to function in a healthy and sustainable manner, serving the interests of storage users and providers alike. This is where blockchain integration comes in.

It is blockchain's ability to chronicle events in a decentralized and immutable manner, that we shall use during the process of assigning storage capacity on a distributed network, as well as the facility to proportion financial rewards in a programmatic and verifiable way, that we'll use to reward storage providers, that makes blockchain so fundamental to Shift's technology. The first step in blockchain integration to be included in our upcoming release, is thus the ability to LOCK tokens as a means of staking a claim to a proportion of the pool of available storage space, as well as the provision of a PIN function for assigning content the status necessary to render it censorship resistant. While not included in our upcoming releases, once storage space is acquired and content pinned, subsequent releases will add the consensus checking used to maintain the state where if one of the three peers responsible for the content's pinning went offline, it would be automatically redistributed to a new peer on the Phoenix Cluster.

In order for a user to store data on our platform, it will be necessary for them to first acquire SHIFT tokens to stake a claim to the amount of storage space needed to host that data. Following this, those SHIFT can be locked using the Shift Nano wallet, and a small fee paid to pin that data permanently (or until the data is unpinned by the wallet holder). These two transaction types can also be conducted in the inverse, serving to undo the prior actions. Put simply, the four transaction types to be debuted in our upcoming release are as follows:

- A LOCK transaction, that sends a designated amount of SHIFT tokens to a virtual wallet where they are stored as a form of collateral, guaranteeing the corresponding amount of storage space is available to the wallet holder.
- An UNLOCK transaction, that returns the debited tokens and releases storage space back to the storage cluster's data pool.
- A PIN transaction, that creates a record on the mainchain containing the asset hash and asset size as data entries allowing only the wallet holder to dictate the data's distribution across the cluster.
- An UNPIN transaction, that creates a record on the mainchain that is read by the cluster as a cancelation of the relevant PIN transaction, and instructs it to free the user's storage space, allowing them to grant it to other assets.

Rob has been working tirelessly over the last few months to carry out the highly technical task of integrating these transactions with our blockchain. It was the complexity of this coding that unfortunately meant that we did not meet our deadline of September 30th for the release of the first iteration of our technology solution to the testnet. Nevertheless, we intend using the time left available to us this year to extensively test all of the functionalities on our private network, with a rescheduled testnet release of our decentralized storage and web hosting solution coming in late-December, 2018.

Our Pricing Model

While we were unable to meet our ambitious release target of the end of Q3, we concluded the quarter by putting the finishing touches to the dynamic, formula-driven pricing model that our platform will use to govern the quantity of SHIFT tokens required to procure storage space. While we provided the community with a very in-depth explanation of how it will work as part of a development update released in October,[8] as it will be integral in the operation of the Shift platform, the essence of how it functions does warrant some description.

The pricing model cannot be understood without reference to the mechanics of the LOCK transaction, the transaction through which the SHIFT token acquires its primary role. Tokens must be locked using a LOCK transaction that, in making those tokens unavailable for other uses, functions as a request for a proportion of the storage capacity of the IPFS swarm. Drive space will only remain available to the storage user for as long as their tokens remain locked, with an UNLOCK transaction being required in order to free the tokens and return the drive space to the platform's available pool. The amount of SHIFT tokens one must lock in order to receive any given number of bytes of hard drive capacity is the product of the following mathematical formula:

$$P = C * (X / Y) * Z * R$$

- P = [SHIFT] = Amount of tokens to lock for Z amount of drive space.
- C = [dimensionless] = Constant.
- X = [byte] = Total amount of the platform's drive space that is claimed (demand).
- Y = [byte] = Total amount of the platform's drive space that is on offer (supply).
- Z = [byte] = Amount of drive space requested by user.
- R = [SHIFT/byte] = Pre-initiated token/byte ratio (conversion factor).

[8] https://www.shiftproject.com/news/news-item/13

This formula-based pricing model will require a great deal of testing to ensure that it meets the expectations of both storage users and storage providers, but we at Shift presently believe that the benefits of the formula-driven pricing model have the potential to contribute to the rapid adoption of our services and growth in our network. Automating the process of price determination through mathematics and thus removing the necessity that storage users and providers need to actively participate in a marketplace, may be an excellent means of removing the barrier to entry that might otherwise exist were newcomers to be faced with an elaborate trading platform.

Once this financial system is successfully tested and deployed, the complementary task of finalizing the means by which storage providers will be rewarded for their services will begin. That task will entail implementing a control mechanism to verify that they're correctly hosting the content that the network has assigned them, as well as enabling a dynamic block reward model that will distribute a quantity of each block reward to those that successfully and consistently pass the verification process.

Q4 2018 - What's to come?

And now we arrive at the present.

During the first half of Q4, we made important enhancements to Phoenix's source code necessary to set up the stable test cluster that is now hosting our project website. During the last week, we on the core team have also been busy creating a final 'to-do list' of the tasks remaining to see the blockchain integration component finalized. Once these are done, we aim to release the decentralized storage and web hosting solution prior to the conclusion of this quarter.

From our user's perspective, the release will come in the form of a rebuilt Shift Nano wallet, that will have a reworked user interface—surpassing that of the Phantom dApp in terms of ease of use and available functions—in addition to the Phoenix node software used to participate in our network as a storage provider being made publicly available. An install script and tutorial explaining Phoenix will also be made public, so that anyone will be able to easily set up their own node and take part in our testing environment by sharing storage capacity. Testnet tokens will then be distributed so that interested parties can participate in the testing of our product, free of charge. We shall be reserving larger quantities of tokens for special partners, however, so that they are able to ensure that the infrastructure meets the requirements of their enterprise use cases.

To coincide with the release of the storage solution, we will announce a major partnership. More partnerships are likely to follow in the wake of this, as no such storage solution that is capable of delivering the performance of ours yet exists. The plan following the launch will then be the development of useful platform mechanics, such as blockchain validation on storage rewards, and, should the launch result in us securing additional financial investment, the completion of a detailed technical white paper outlining a re-architecturing of the Shift platform able to deliver us a consensus algorithm and blockchain core better suited to the needs of a rapidly expanding Shift ecosystem.

With this promising vision in mind, we would like to end this summary with a big thank you to Rob and Craig for their contributions to the realization of such groundbreaking technology. They have been working extremely hard throughout the past year, though things have been far from easy in terms of the predominant market sentiment. We would like to emphasize that they have been managing multiple roles in order to serve the Shift Project, in addition to other commitments, with their passion and not immediate financial reward carrying them through this considerable endeavor. None of us would be investing our time and other resources were it not for our continued belief that what we are working on may become one of the greatest achievements in the cryptocurrency scene, as well as the broader movement to decentralize the Web, and, in doing so, protect knowledge and the means of its transmission from the threat of undue censorship.

Sincerely,

Ralf S. (President / Lead Developer)

Werner Heisenberg (Vice President / Operations Manager)

For more information,

visit www.shiftproject.com